Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Finite Fields and Their Applications 10 (2004) 566–582
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

p-Ary and q-ary versions of certain results about bent functions and resilient functions

Xiang-Dong Hou*,[1]

Department of Mathematics and Statistics, Wright State University, 3640 Colonel Glenn Hwy, Dayton, OH 45435-001, USA

Received 2 July 2003; revised 1 December 2003

Communicated by Stephen D. Cohen

Abstract

Using the Teichmüller character and Gauss sums, we obtain the following results concerning p-ary bent functions and q-ary resilient functions: (1) a characterization of certain q-ary resilient functions in terms of their coefficients; (2) stronger upper bounds for the degree of p-ary bent functions; (3) determination of all bent functions on $\mathbb{F}_p$; (4) a characterization of ternary weakly regular bent functions in terms of their coefficients.

Keywords: Bent function; Gauss sum; Resilient function; Techmüller character

1. Introduction

Let p be a prime and $q = p^s$. Denote the set of all functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ by $\mathscr{F}(\mathbb{F}_q^n, \mathbb{F}_q)$. As an $\mathbb{F}_q$-algebra,

$$\mathscr{F}(\mathbb{F}_q^n, \mathbb{F}_q) = \mathbb{F}_q[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n).$$

Let $U = \{0, 1, \ldots, q-1\}^n$. For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ and $\mathbf{u} = (u_1, \ldots, u_n) \in U$, define $\mathbf{x}^{\mathbf{u}} = x_1^{u_1} \cdots x_n^{u_n}$. Then every $f \in \mathscr{F}(\mathbb{F}_q^n, \mathbb{F}_q)$ is uniquely of the form

$$f(\mathbf{x}) = \sum_{\mathbf{u} \in U} a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}}, \quad a_{\mathbf{u}} \in \mathbb{F}_q. \tag{1.1}$$

*Fax: +937-775-2081.
E-mail address: xhou@tarski.math.usf.edu, xhou@cas.usf.edu.
[1] Present address: Department of Mathematics, University of South Florida, Tampa, FL 33620 USA.

1071-5797/$ - see front matter
doi:10.1016/j.ffa.2003.12.004

Let $\zeta \in \mathbb{C}$ be a primitive pth root of unity. The Fourier transform of f at $\mathbf{c} \in \mathbb{F}_q^n$ is

$$\hat{f}(\mathbf{c}) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} \zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f(\mathbf{x})+\mathbf{c}\cdot\mathbf{x})},$$

where $\mathbf{c} \cdot \mathbf{x}$ is the standard dot product. For $\mathbf{x} \in \mathbb{F}_q^n$ and $\mathbf{u} \in U$, we use $|\mathbf{x}|$ and $|\mathbf{u}|$ to denote their Hamming weights, i.e., the numbers of nonzero components in $\mathbf{x}$ and $\mathbf{u}$.

This paper is concerned with the following two known results.

Theorem 1.1. *Let $q = 2$ and let $f \in \mathscr{F}(\mathbb{F}_2^n, \mathbb{F}_2)$ be of the form*

$$f(\mathbf{x}) = \sum_{i=1}^{m} \mathbf{x}^{\mathbf{u}_i}, \tag{1.2}$$

where $\mathbf{u}_1, \ldots, \mathbf{u}_m \in U$ are distinct. Let t be a positive integer. Then

$$\hat{f}(\mathbf{c}) = 0 \quad \textit{for all } \mathbf{c} \in \mathbb{F}_2^n \quad \textit{with } |\mathbf{c}| \geqslant t$$

if and only if

$$\sum_{\substack{0 \leqslant t_1, \ldots, t_m \leqslant 1 \\ t_1\mathbf{u}_1 \oplus \cdots \oplus t_m\mathbf{u}_m = \mathbf{u}}} (-2)^{t_1+\cdots+t_m} = 0 \quad \textit{for all } \mathbf{u} \in U \textit{ with } |\mathbf{u}| \geqslant t. \tag{1.3}$$

(*In* (1.3), *the operation $\oplus$ on $U = \{0,1\}^n$ is defined componentwise by the rules that $0 \oplus 0 = 0$ and that $u \oplus v = 1$ if u and v are not both* 0.)

Theorem 1.2. *Let $f \in \mathscr{F}(\mathbb{F}_2^n, \mathbb{F}_2)$ be as in* (1.2) *and let v_2 be the 2-adic order function. Then*

$$v_2(\hat{f}(\mathbf{c}) - \hat{f}(0)) > v_2(\hat{f}(0)) \quad \textit{for all } \mathbf{c} \in \mathbb{F}_2^n$$

if and only if

$$v_2\left(\sum_{\substack{0 \leqslant t_1, \ldots, t_m \leqslant 1 \\ t_1\mathbf{u}_1 \oplus \cdots \oplus t_m\mathbf{u}_m = \mathbf{u}}} (-2)^{t_1+\cdots+t_m} \right) > v_2(\hat{f}(0)) - n + |\mathbf{u}|$$

for all $(1, \ldots, 1) \neq \mathbf{u} \in U$.

Theorem 1.1 is a combination of Proposition 1 of [4] and a result of [3]. A binary function $f \in \mathscr{F}(\mathbb{F}_2^n, \mathbb{F}_2)$ is called t-resilient if

$$\hat{f}(\mathbf{c}) = 0 \quad \text{for all } \mathbf{c} \in \mathbb{F}_2^n \quad \text{with } |\mathbf{c}| \leqslant t.$$

Resilient functions are used in cryptosystems to enhance resistance against correlation attacks [10]. Observe that the functions f in Theorem 1.1 are precisely

the ones such that $f(\mathbf{x})+(1,\ldots,1)\cdot\mathbf{x}$ is a binary $(n-t)$-resilient function. Hence Theorem 1.1 is actually a characterization of binary resilient functions in terms of the coefficients in their polynomial form (1.1).

Theorem 1.2 is not explicitly stated in the literature. However, it follows from the results of [3] and is thus considered known. A binary function $f\in\mathscr{F}(\mathbb{F}_2^n,\mathbb{F}_2)$ is called bent if $\hat{f}(\mathbf{c})=\pm 2^{n/2}$ for all $\mathbf{c}\in\mathbb{F}_2^n$. ($n$ must be even.) It is known that $f\in\mathscr{F}(\mathbb{F}_2^n,\mathbb{F}_2)$ is bent if and only if $v_2(\hat{f}(\mathbf{c}))=\frac{n}{2}$ for all $\mathbf{c}\in\mathbb{F}_2^n$ [2, Lemma 1]. Using Theorem 1.2, one can prove the following characterization of binary bent functions. (Also see [4, Theorem 3.1].)

Corollary 1.3. *Let n be even and $f\in\mathscr{F}(\mathbb{F}_2^n,\mathbb{F}_2)$ be as in* (1.2). *Then f is bent if and only if*

$$v_2\left(\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant 1\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}}}(-2)^{t_1+\cdots+t_m}\right)\begin{cases}=\frac{n}{2} & \text{if } \mathbf{u}=(1,\ldots,1),\\ >|\mathbf{u}|-\frac{n}{2}, & \text{if } \mathbf{u}\neq(1,\ldots,1),\end{cases}$$

for all $\mathbf{u}\in U$.

It is natural to ask what the q-ary versions of Theorems 1.1 and 1.2 are. We will state and prove the q-ary versions of Theorems 1.1 and 1.2 in Sections 3 and 4. The tools of our proofs are the Teichmüller character of p-adic fields and Gauss sums. When $q=2$, the Teichmüller character and Gauss sums are trivial; such trivialities contribute to the fact that the sums in Theorems 1.1 and 1.2 are rather simple.

We will recall the basic facts about the Teichmüller character and Gauss sums in Section 2. In Section 4, after proving the q-ary version of Theorem 1.2, we apply the result to p-ary bent functions. We improve an upper bound for the degree of p-ary bent functions obtained in [8]. We show that for odd prime p, bent functions in $\mathscr{F}(\mathbb{F}_p,\mathbb{F}_p)$ are precisely quadratic functions. We also prove a characterization for ternary weakly regular bent functions in terms of their coefficients. The ternary case appears to be the only instance where Corollary 1.3 can be generalized.

2. Techmüller character and Gauss sums

Details of the materials in this section can be found in Chapter IV of [6], Chapter 1 of [7] and [1].

Let $K/\mathbb{Q}_p$ be an unramified extension of degree s. Let ζ' be a primitive pth root of unity in some extension of K. Then $K(\zeta')/K$ is totally ramified of degree $p-1$ and $\zeta'-1$ is the prime of $K(\zeta')$. Let v_p be the p-adic order function of $K(\zeta')$ normalized such that $v_p(p)=1$. Let $\zeta\in\mathbb{C}$ be a primitive pth root of unity. The cyclotomic extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ has only one prime ideal $\mathfrak{p}=(\zeta-1)\mathbb{Z}[\zeta]$ above the prime ideal $p\mathbb{Z}$ of $\mathbb{Q}$ and $p\mathbb{Z}[\zeta]=\mathfrak{p}^{p-1}$. The p-adic order on $\mathbb{Q}$ can be extended to $\mathbb{Q}(\zeta)$ by setting

$v_p = \frac{1}{p-1} v_{\mathfrak{p}}$, where $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic order on $\mathbb{Q}(\zeta)$. The cyclotomic filed $\mathbb{Q}(\zeta)$ is embedded in $K(\zeta')$ with ζ identified with ζ'; the p-adic order functions of $\mathbb{Q}(\zeta)$ and $K(\zeta')$ coincide on $\mathbb{Q}(\zeta)$. In what follows, we will not distinguish between ζ and ζ'.

Let $\mathfrak{o}_{K(\zeta)}$ be the ring of integers of $K(\zeta)$. The residue field of $K(\zeta)$ is $\mathfrak{o}_{K(\zeta)}/(\zeta - 1)\mathfrak{o}_{K(\zeta)} = \mathbb{F}_q$ where $q = p^s$. Denote by T the Teichmüller set of $K(\zeta)$. The Teichmüller character of $K(\zeta)$ is the map $\omega : \mathbb{F}_q \ (= \mathfrak{o}_{K(\zeta)}/(\zeta - 1)\mathfrak{o}_{K(\zeta)}) \to T$ defined by

$$\omega(\bar{x}) = \lim_{l \to +\infty} x^{q^l}, \quad x \in \mathfrak{o}_{K(\zeta)},$$

where $\bar{x}$ is the image of x in $\mathfrak{o}_{K(\zeta)}/(\zeta - 1)\mathfrak{o}_{K(\zeta)}$.

For each $t \in \mathbb{Z}$ (or $\mathbb{Z}/(q-1)\mathbb{Z}$), the Gauss sum $g(t)$ is defined by

$$g(t) = -\sum_{x \in \mathbb{F}_q^*} (\omega(x))^{-t} \zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}.$$

We have (cf. [1])

$$\zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)} = \sum_{t=0}^{q-1} G(t)(\omega(x))^t \quad \text{for all } x \in \mathbb{F}_q, \tag{2.1}$$

where

$$G(t) = \begin{cases} 1 & \text{if } t = 0, \\ \frac{q}{1-q} & \text{if } t = q-1, \\ \frac{1}{1-q} g(t) & \text{if } 0 < t < q-1. \end{cases}$$

For each integer $t \geqslant 0$ written in the p-adic expansion $t = t_0 p^0 + t_1 p^1 + \cdots$, where $0 \leqslant t_i \leqslant p-1$, define

$$S_p(t) = t_0 + t_1 + \cdots.$$

The Stickelberger theorem states that

$$v_p(G(t)) = \frac{1}{p-1} S_p(t) \quad \text{for } 0 \leqslant t \leqslant q-1.$$

We briefly describe the roles of the Teichmüller character and Gauss sums in our approach. For the function $f \in \mathscr{F}(\mathbb{F}_q^n, \mathbb{F}_q)$ given in (1.1), we try to express its Fourier transform $\hat{f}(\mathbf{c})$ in terms of its coefficients $a_{\mathbf{u}}$. Although $\hat{f}(\mathbf{c}) \in \mathbb{Q}(\zeta)$, the formula for $\hat{f}(\mathbf{c})$ in terms of $a_{\mathbf{u}}$ is realized in the extension $K(\zeta)$ of $\mathbb{Q}(\zeta)$. In this formula, $a_{\mathbf{u}}$ appears in the form of the Teichmüller character coupled with Gauss sums. The Stickelberger theorem enables us to relate the p-adic order $v_p(\hat{f}(\mathbf{c}))$ to the coefficients $a_{\mathbf{u}}$.

3. The q-ary Version of Theorem 1.1

We first define an operation $\oplus$ in $\{0,1,\ldots,q-1\}$ using the rules that $0\oplus 0=0$ and that $u\oplus v=$ the modulo $q-1$ representative of $u+v$ in $\{1,\ldots,q-1\}$ if u and v are not both 0. Extend $\oplus$ to $U=\{0,1,\ldots,q-1\}^n$ through components. In fact, for $\mathbf{u},\mathbf{v}\in U$, $\mathbf{x}^{\mathbf{u}}\mathbf{x}^{\mathbf{v}}=\mathbf{x}^{\mathbf{u}+\mathbf{v}}$ for all $\mathbf{x}\in\mathbb{F}_q^n$. Also define a partial order $\prec$ on U as follows. For $\mathbf{u}=(u_1,\ldots,u_n)$ and $\mathbf{v}=(v_1,\ldots,v_n)$ in U, we say $\mathbf{u}\prec\mathbf{v}$ if for each $1\leqslant i\leqslant n$, $u_i=v_i$ or $(u_i,v_i)=(0,q-1)$.

Let $f\in\mathscr{F}(\mathbb{F}_q^n,\mathbb{F}_q)$ be written in the form

$$f(\mathbf{x})=\sum_{i=1}^{m}a_i\mathbf{x}^{\mathbf{u}_i}, \tag{3.1}$$

where $\mathbf{u}_1,\ldots,\mathbf{u}_m\in U$ are distinct and $0\neq a_i\in\mathbb{F}_q$. By (2.1), we have

$$\begin{aligned}\zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f(\mathbf{x}))}&=\prod_{i=1}^{m}\zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a_i\mathbf{x}^{\mathbf{u}_i})}\\&=\prod_{i=1}^{m}\sum_{t_i=0}^{q-1}G(t_i)\omega(a_i^{t_i}\mathbf{x}^{t_i\mathbf{u}_i})\\&=\sum_{\mathbf{u}\in U}\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant q-1\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}}}G(t_1)\cdots G(t_m)\omega(a_1^{t_1}\cdots a_m^{t_m})\omega(\mathbf{x}^{\mathbf{u}})\\&=\sum_{\mathbf{u}\in U}h_f(\mathbf{u})\omega(\mathbf{x}^{\mathbf{u}}),\end{aligned} \tag{3.2}$$

where

$$h_f(\mathbf{u})=\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant q-1\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}}}G(t_1)\cdots G(t_m)\omega(a_1^{t_1}\cdots a_m^{t_m}). \tag{3.3}$$

Remarks. (i) In fact, $\omega(\mathbf{x}^{\mathbf{u}})$ ($\mathbf{u}\in U$) form a basis for the $\mathfrak{o}_{K(\zeta)}$-algebra of all functions from $\mathbb{F}_q^n$ to $\mathfrak{o}_{K(\zeta)}$. Thus, $h_f(\mathbf{u})$ are the coefficients of $\zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f(\mathbf{x}))}$ with respect to this basis.

(ii) In Theorems 1.1 and 1.2, and Corollary 1.3, the sum

$$\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant 1\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}}}(-2)^{t_1+\cdots+t_m}$$

is actually $h_f(\mathbf{u})$ with $q=2$.

For $\mathbf{u} = (u_1, \ldots, u_n) \in U$, define

$$H_f(\mathbf{u}) = g(-u_1)\cdots g(-u_n)(q-1)^{|\{k:u_k \neq 0\}|} q^{|\{k:u_k=0\}|} h_f(\mathbf{u}). \tag{3.4}$$

Lemma 3.1. *Let* $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ *whose nonzero components are* $c_{i_1}, \ldots, c_{i_a}$. *Then*

$$\hat{f}(\mathbf{c}) = (1-q)^{-a} \sum_{\mathbf{u}} \omega(c_{i_1}^{-u_{i_1}} \cdots c_{i_a}^{-u_{i_a}}) H_f(\mathbf{u}), \tag{3.5}$$

where the sum is over all $\mathbf{u} = (u_1, \ldots, u_n) \in U$ *such that*

$$u_i \in \begin{cases} \{1, \ldots, q-1\} & \text{if } i \in \{i_1, \ldots, i_a\}, \\ \{0, q-1\} & \text{if } i \notin \{i_1, \ldots, i_a\}. \end{cases}$$

Proof. Without loss of generality, let $\mathbf{c} = (c_1, \ldots, c_a, 0, \ldots, 0)$ where $c_1, \ldots, c_a$ are nonzero. By (3.2), we have

$$\begin{aligned} \hat{f}(\mathbf{c}) &= \sum_{\mathbf{x} \in \mathbb{F}_q^n} \zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f(\mathbf{x}))} \zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbf{c}\cdot\mathbf{x})} \\ &= \sum_{\mathbf{x} \in \mathbb{F}_q^n} \zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbf{c}\cdot\mathbf{x})} \sum_{\mathbf{u} \in U} h_f(\mathbf{u}) \omega(\mathbf{x}^{\mathbf{u}}) \\ &= \sum_{\mathbf{u} \in U} h_f(\mathbf{u}) \sum_{\mathbf{x} \in \mathbb{F}_q^n} \omega(\mathbf{x}^{\mathbf{u}}) \zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbf{c}\cdot\mathbf{x})}. \end{aligned} \tag{3.6}$$

In general, for $\mathbf{u} = (u_1, \ldots, u_n) \in U$,

$$\begin{aligned} &\sum_{\mathbf{x} \in \mathbb{F}_q^n} \omega(\mathbf{x}^{\mathbf{u}}) \zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbf{c}\cdot\mathbf{x})} \\ &= \begin{cases} (-1)^a g(-u_1)\cdots g(-u_a)\omega(c_1^{-u_1}\cdots c_a^{-u_a})(q-1)^{n-a-|\{k:u_k=0\}|} q^{|\{k:u_k=0\}|} \\ \qquad \text{if } u_1, \ldots, u_a \neq 0, u_{a+1}, \ldots, u_n = 0 \text{ or } q-1, \\ 0 \qquad \text{otherwise.} \end{cases} \end{aligned} \tag{3.7}$$

Eq. (3.5) follows from (3.6), (3.7) and (3.4) immediately. □

Lemma 3.2. *Let* $\mathbf{u} = (u_1, \ldots, u_n) \in U$ *whose nonzero components are* $u_{i_1}, \ldots, u_{i_a}$. *Then*

$$\sum_{\mathbf{c}} \hat{f}(\mathbf{c}) \omega(\mathbf{c}^{\mathbf{u}}) = (-1)^a \sum_{\mathbf{v} \succ \mathbf{u}} H_f(\mathbf{v}), \tag{3.8}$$

where the sum on the left-hand side of (3.8) *is over all* $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ *such that*

$$c_i \begin{cases} \neq 0 & \text{if } i \in \{i_1, \ldots, i_a\}, \\ = 0 & \text{if } i \notin \{i_1, \ldots, i_a\}. \end{cases} \tag{3.9}$$

Proof. We may assume $\mathbf{u} = (u_1, \ldots, u_a, 0, \ldots, 0)$ where $u_1, \ldots, u_a$ are nonzero. By Lemma 3.1,

$$\sum_{\mathbf{c}} \hat{f}(\mathbf{c})\omega(\mathbf{c}^{\mathbf{u}}) = (1-q)^{-a} \sum_{\mathbf{v}} H_f(\mathbf{v}) \sum_{\mathbf{c}} \omega(c_1^{u_1-v_1} \cdots c_a^{u_a-v_a}),$$

where $\mathbf{c}$ runs over $(\mathbb{F}_q^*)^a \times \{0\}^{n-a}$ and $\mathbf{v} = (v_1, \ldots, v_n)$ runs over $\{1, \ldots, q-1\}^a \times \{0, q-1\}^{n-a}$. Note that for $\mathbf{v} \in \{1, \ldots, q-1\}^a \times \{0, q-1\}^{n-a}$,

$$\sum_{\mathbf{c}} \omega(c_1^{u_1-v_1} \cdots c_a^{u_a-v_a}) = \begin{cases} (q-1)^a & \text{if } \mathbf{v} \succ \mathbf{u}, \\ 0 & \text{otherwise.} \end{cases}$$

Hence, we have

$$\sum_{\mathbf{c}} \hat{f}(\mathbf{c})\omega(\mathbf{c}^{\mathbf{u}}) = (-1)^a \sum_{\mathbf{v} \succ \mathbf{u}} H_f(\mathbf{v}). \qquad \square$$

Theorem 3.3 (The q-ary version of Theorem 1.1). *Let $f \in \mathscr{F}(\mathbb{F}_q^n, \mathbb{F}_q)$ and let t be a positive integer. The following two conditions are equivalent*:

(i) $\hat{f}(\mathbf{c}) = 0$ *for all* $\mathbf{c} \in \mathbb{F}_q^n$ *with* $|\mathbf{c}| \geqslant t$.
(ii) $h_f(\mathbf{u}) = 0$ *for all* $\mathbf{u} \in U$ *with* $|\mathbf{u}| \geqslant t$.

Proof. (i) $\Rightarrow$ (ii). Let

$$L_f(\mathbf{u}) = \sum_{\mathbf{v} \succ \mathbf{u}} H_f(\mathbf{v}), \quad \mathbf{u} \in U.$$

Then

$$H_f(\mathbf{u}) = \sum_{\mathbf{v} \succ \mathbf{u}} \mu(\mathbf{u}, \mathbf{v}) L_f(\mathbf{v}), \quad \mathbf{u} \in U, \tag{3.10}$$

where μ is the Möbius function of the partially ordered set $(U, \prec)$. (In fact, if $\mathbf{u} \prec \mathbf{v}$, then $\mu(\mathbf{u}, \mathbf{v}) = (-1)^{d(\mathbf{u},\mathbf{v})}$, where $d(\mathbf{u}, \mathbf{v})$ is the Hamming distance between $\mathbf{u}$ and $\mathbf{v}$.)

Condition (i) and Eq. (3.8) imply that $L_f(\mathbf{u}) = 0$ for all $\mathbf{u} \in U$ with $|\mathbf{u}| \geqslant t$. By (3.10), we have $H_f(\mathbf{u}) = 0$ for all $\mathbf{u} \in U$ with $|\mathbf{u}| \geqslant t$, which is equivalent to (ii).

(ii) $\Rightarrow$ (i). We have $H_f(\mathbf{u}) = 0$ for all $\mathbf{u} \in U$ with $|\mathbf{u}| \geqslant t$. By Lemma 3.1, $\hat{f}(\mathbf{c}) = 0$ for all $\mathbf{c} \in \mathbb{F}_q^n$ with $|\mathbf{c}| \geqslant t$. $\square$

Remark. A q-ary function $f \in \mathscr{F}(\mathbb{F}_q^n, \mathbb{F}_q)$ is called t-resilient if $\hat{f}(\mathbf{c}) = 0$ for all $\mathbf{c} \in \mathbb{F}_q^n$ with $|\mathbf{c}| \leqslant t$. The functions f satisfying the conditions in Theorem 3.3 are precisely the ones such that $f(\mathbf{x}) + \mathbf{c} \cdot \mathbf{x}$ is $(n-t)$-resilient for all $\mathbf{c} \in \mathbb{F}_q^n$ with $|\mathbf{c}| = n$.

4. The q-ary version of Theorem 4.1

Theorem 4.1. *Let $f \in \mathscr{F}(\mathbb{F}_q^n, \mathbb{F}_q)$. Let $\alpha \in K(\zeta)$ and $\varepsilon \geqslant 0$ such that $v_p(q\alpha) \geqslant \varepsilon$. Then the following two conditions are equivalent*:

(i) $v_p(\hat{f}(\mathbf{c}) - \alpha) \geqslant \varepsilon$ *for all* $\mathbf{c} \in \mathbb{F}_q^n$.

(ii)
$$v_p(h_f(q-1, \ldots, q-1) - (-1)^n\alpha) \geqslant \varepsilon \tag{4.1}$$

and

$$v_p(h_f(\mathbf{u})) \geqslant \varepsilon - ns + \frac{1}{p-1}(S_p(u_1) + \cdots + S_p(u_n)) \tag{4.2}$$

for all $(q-1, \ldots, q-1) \neq \mathbf{u} = (u_1, \ldots, u_n) \in U$. (*In* (4.2), $s = \log_p q$.)

Proof. (i) $\Rightarrow$ (ii). If $\mathbf{u} \in U \backslash \{0, q-1\}^n$, then by (3.8),

$$\sum_{\mathbf{c}} (\hat{f}(\mathbf{c}) - \alpha)\omega(\mathbf{c}^{\mathbf{u}}) = (-1)^{|\mathbf{u}|} \sum_{\mathbf{v} \succ \mathbf{u}} H_f(\mathbf{v}),$$

where the range of $\mathbf{c}$ is described in (3.9). Therefore,

$$v_p\left(\sum_{\mathbf{v} \succ \mathbf{u}} H_f(\mathbf{v})\right) \geqslant \varepsilon \quad \text{for all } \mathbf{u} \in U \backslash \{0, q-1\}^n. \tag{4.3}$$

If $\mathbf{u} \in \{0, q-1\}^n$, also by (3.8),

$$\sum_{\mathbf{c}} (\hat{f}(\mathbf{c}) - \alpha)\omega(\mathbf{c}^{\mathbf{u}}) = (-1)^{|\mathbf{u}|} \sum_{\mathbf{v} \succ \mathbf{u}} H_f(\mathbf{v}) - (q-1)^{|\mathbf{u}|}\alpha. \tag{4.4}$$

Since $v_p(q\alpha) \geqslant \varepsilon$, we have $v_p((q-1)^{|\mathbf{u}|}\alpha - (-1)^{|\mathbf{u}|}\alpha) \geqslant \varepsilon$. Condition (i) and Eq. (4.4) imply that

$$v_p\left(\sum_{\mathbf{v} \succ \mathbf{u}} H_f(\mathbf{v}) - \alpha\right) \geqslant \varepsilon \quad \text{for all } \mathbf{u} \in \{0, q-1\}^n. \tag{4.5}$$

Let $\mathbf{u} = (q-1, \ldots, q-1)$ in (4.5), we have $v_p(H_f(q-1, \ldots, q-1) - \alpha) \geqslant \varepsilon$, which is equivalent to (4.1). Therefore,

$$v_p\left(\sum_{\substack{\mathbf{v} \succ \mathbf{u} \\ \mathbf{v} \neq (q-1, \ldots, q-1)}} H_f(\mathbf{v})\right) \geqslant \varepsilon \quad \text{for all } \mathbf{u} \in \{0, q\}^n \backslash \{(q-1, \ldots, q-1)\}. \tag{4.6}$$

Combine (4.3) and (4.6) as

$$v_p\left(\sum_{\substack{\mathbf{v}\succ\mathbf{u}\\ \mathbf{v}\neq(q-1,\ldots,q-1)}} H_f(\mathbf{v})\right)\geqslant\varepsilon \quad \text{for all } (q-1,\ldots,q-1)\neq\mathbf{u}\in U.$$

A Möbius inversion in $(U\backslash\{(q-1,\ldots,q-1)\},\prec)$ gives

$$v_p(H_f(\mathbf{u}))\geqslant\varepsilon \quad \text{for all } (q-1,\ldots,q-1)\neq\mathbf{u}\in U.$$

Observe from (3.4) that

$$\begin{aligned} v_p(H_f(\mathbf{u})) &= v_p(G(q-1-u_1)\cdots G(q-1-u_n)) + v_p(h_f(\mathbf{u}))\\ &= \frac{1}{p-1}(S_p(q-1-u_1)+\cdots+S_p(q-1-u_n)) + v_p(h_f(\mathbf{u}))\\ &= ns - \frac{1}{p-1}(S_p(u_1)+\cdots+S_p(u_n)) + v_p(h_f(\mathbf{u})). \end{aligned}$$

Therefore, (4.2) follows.

(ii) $\Rightarrow$ (i). Inequalities (4.1) and (4.2) imply that $v_p(H_f(q-1,\ldots,q-1)-\alpha)\geqslant\varepsilon$ and that $v_p(H_f(\mathbf{u}))\geqslant\varepsilon$ for all $(q-1,\ldots,q-1)\neq\mathbf{u}\in U$. It follows immediately from (3.5) that

$$v_p(\hat{f}(\mathbf{c})-\alpha)\geqslant\varepsilon \quad \text{for all } \mathbf{c}\in\mathbb{F}_q^n. \qquad \square$$

Lemma 4.2. *Let $f\in\mathscr{F}(\mathbb{F}_q^n,\mathbb{F}_q)$ and $\varepsilon\geqslant 0$. If*

$$v_p(h_f(\mathbf{u}))\geqslant\varepsilon - ns + \frac{1}{p-1}(S_p(u_1)+\cdots+S_p(u_n)) \tag{4.7}$$

for all $(q-1,\ldots,q-1)\neq\mathbf{u}=(u_1,\ldots,u_n)\in U$, then

$$v_p\left(h_f(q-1,\ldots,q-1)-\frac{1}{(q-1)^n}\hat{f}(0)\right)\geqslant\varepsilon. \tag{4.8}$$

Proof. Inequality (4.7) gives

$$v_p(H_f(\mathbf{u}))\geqslant\varepsilon \quad \text{for all } (q-1,\ldots,q-1)\neq\mathbf{u}\in U.$$

Therefore, by (3.5),

$$\hat{f}(0) \equiv H_f(q-1,\ldots,q-1) \pmod{p^{\varepsilon}}$$
$$= (q-1)^n h_f(q-1,\ldots,q-1)$$

which is equivalent to (4.8). □

Corollary 4.3 (The q-ary version of Theorem 1.2). *Let $f \in \mathscr{F}(\mathbb{F}_q^n, \mathbb{F}_q)$. Then the following two conditions are equivalent*:

(i) $v_p(\hat{f}(\mathbf{c}) - \hat{f}(0)) > v_p(\hat{f}(0))$ *for all* $\mathbf{c} \in \mathbb{F}_q^n$.

(ii)
$$v_p(h_f(\mathbf{u})) > v_p(\hat{f}(0)) - ns + \frac{1}{p-1}(S_p(u_1) + \cdots + S_p(u_n)) \tag{4.9}$$

for all $(q-1,\ldots,q-1) \neq \mathbf{u} = (u_1,\ldots,u_n) \in U$.

Proof. Let $\alpha = \hat{f}(0)$ and $\varepsilon = v_p(\alpha) + \frac{1}{p-1}$. (Note that $v_p(q\alpha) \geqslant \varepsilon$.) Observe that condition (i) of Corollary 4.3 is equivalent to condition (i) of Theorem 4.1 and that inequality (4.9) is equivalent to (4.2) in Theorem 4.1. Therefore, we only have to show that (4.9) implies (4.1) in Theorem 4.1. This implication is given by Lemma 4.2. □

An $f \in \mathscr{F}(\mathbb{F}_p^n, \mathbb{F}_p)$ is called a p-ary bent function if

$$|\hat{f}(\mathbf{c})| = p^{\frac{n}{2}} \quad \text{for all } \mathbf{c} \in \mathbb{F}_p^n$$

[5]. It is well known that the maximal degree of binary bent functions in $\mathscr{F}(\mathbb{F}_2^n, \mathbb{F}_2)$ ($n \geqslant 4$ even) is $\frac{n}{2}$ [9]. The maximal degree of p-ary bent functions is not known. It was proved in [8] that if $f \in \mathscr{F}(\mathbb{F}_p^n, \mathbb{F}_p)$ is bent, then

$$\deg f \leqslant (p-1)\left(\left\lfloor \frac{n}{2} \right\rfloor + 2\right) - 1. \tag{4.10}$$

The following proposition is an improvement of (4.10).

Proposition 4.4. *Let $f \in \mathscr{F}(\mathbb{F}_p^n, \mathbb{F}_p)$ be a bent function. Then*

$$\deg f \leqslant \frac{(p-1)n}{2} + 1. \tag{4.11}$$

Proof. Since complex conjugation in $\mathbb{Q}(\zeta)$ preserves the p-adic order, we have

$$v_p(\hat{f}(\mathbf{c})) = \frac{n}{2} \quad \text{for all } \mathbf{c} \in \mathbb{F}_p^n.$$

Write $f(\mathbf{x}) = \sum_{i=1}^{m} a_i \mathbf{x}^{\mathbf{u}_i}$, where $0 \neq a_i \in \mathbb{F}_p$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m \in U = \{0, 1, \ldots, p-1\}^n$ are distinct. Using Theorem 4.1 with $\alpha = 0$ and $\varepsilon = \frac{n}{2}$, we have

$$v_p(h_f(\mathbf{u})) \geqslant -\frac{n}{2} + \frac{1}{p-1}(u_1 + \cdots + u_n) \tag{4.12}$$

for all $\mathbf{u} = (u_1, \ldots, u_n) \in U$. Without loss of generality, assume that $\mathbf{u}_1 = (u_{11}, \ldots, u_{1n})$ is such that $u_{11} + \cdots + u_{1n} = \deg f$. Letting $\mathbf{u} = \mathbf{u}_1$ in (4.12), we have

$$\begin{aligned} -\frac{n}{2} + \frac{1}{p-1}\deg f &\leqslant v_p(h_f(\mathbf{u}_1)) \\ &= v_p\left(\sum_{\substack{0 \leqslant t_1, \ldots, t_m \leqslant p-1 \\ t_1\mathbf{u}_1 \oplus \cdots \oplus t_m\mathbf{u}_m = \mathbf{u}_1}} G(t_1)\cdots G(t_m)\omega(a_1^{t_1}\cdots a_m^{t_m}) \right) \\ &= v_p(G(1)G(0)\cdots G(0)\omega(a_1^1 a_2^0 \cdots a_m^0)) \\ &= \frac{1}{p-1}. \end{aligned} \tag{4.13}$$

Therefore,

$$\deg f \leqslant \frac{(p-1)n}{2} + 1. \qquad \square$$

In [5], a bent function $f \in \mathscr{F}(\mathbb{F}_p^n, \mathbb{F}_p)$ is called regular if for every $\mathbf{c} \in \mathbb{F}_p^n$, $p^{-n/2}\hat{f}(\mathbf{c})$ is a pth root of unity. We shall call a bent function $f \in \mathscr{F}(\mathbb{F}_p^n, \mathbb{F}_p)$ weakly regular if there is there is a $w \in \mathbb{C}$ with $|w| = 1$ such that $wp^{-n/2}\hat{f}(\mathbf{c})$ is a pth root of unity for all $\mathbf{c} \in \mathbb{F}_p^n$. It appears that all known p-ary bent functions are weakly regular.

Proposition 4.5. *Let $f \in \mathscr{F}(\mathbb{F}_p^n, \mathbb{F}_p)$ be a weakly regular bent function with $(p-1)n \geqslant 4$. Then*

$$\deg f \leqslant \frac{(p-1)n}{2}. \tag{4.14}$$

Proof. We have $v_p(\hat{f}(0)) = \frac{n}{2}$ and

$$v_p(\hat{f}(\mathbf{c}) - \hat{f}(0)) > \frac{n}{2} \quad \text{for all } \mathbf{c} \in \mathbb{F}_p^n,$$

since $v_p(\zeta^i - 1) > 0$ for $i \in \mathbb{Z}$. Let $f(\mathbf{x}) = \sum_{i=1}^{m} a_i \mathbf{x}^{\mathbf{u}_i}$, where $0 \neq a_i \in \mathbb{F}_p$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m \in U$ are distinct. Then by Corollary 4.3,

$$v_p(h_f(\mathbf{u})) > -\frac{n}{2} + \frac{1}{p-1}(u_1 + \cdots + u_n) \tag{4.15}$$

for all $(p-1,\ldots,p-1)\neq\mathbf{u}=(u_1,\ldots,u_n)\in\mathbb{F}_p^n$. Without loss of generality, assume that $\mathbf{u}_1=(u_{11},\ldots,u_{1n})$ is such that $u_{11}+\cdots+u_{1n}=\deg f$.

We first claim that $\mathbf{u}_1\neq(p-1,\ldots,p-1)$. Otherwise,

$$\begin{aligned} v_p(h_f(\mathbf{u}_1)) &= v_p\left(\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant p-1\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}_1}} G(t_1)\cdots G(t_m)\omega(a_1^{t_1}\cdots a_m^{t_m})\right)\\ &= v_p(G(1)G(0)\cdots G(0)\omega(a_1^1a_2^0\cdots a_m^0))\\ &= \frac{1}{p-1}. \end{aligned} \tag{4.16}$$

However, by Lemma 4.2, we have

$$v_p\left(h_f(\mathbf{u}_1)-\frac{1}{(p-1)^n}\hat{f}(0)\right)>\frac{n}{2}$$

which contradicts (4.16) since $\frac{1}{p-1}<\frac{n}{2}$. Therefore $\mathbf{u}_1\neq(p-1,\ldots,p-1)$.

Now we let $\mathbf{u}=\mathbf{u}_1$ in (4.15) and use the same argument in (4.13). Inequality (4.14) follows immediately. □

Remarks. (i) When n is even and $(p-1)n\geqslant 4$, the upper bound (4.14) is attained by the Maiorana–McFarland bent functions [5]. A Maiorana–McFarland bent function $f\in\mathscr{F}(\mathbb{F}_p^n,\mathbb{F}_p)$ is of the form

$$\begin{aligned} f:\mathbb{F}_p^{\frac{n}{2}}\times\mathbb{F}_p^{\frac{n}{2}}&\to\mathbb{F}_p,\\ (\mathbf{x},\mathbf{y})&\mapsto\mathbf{x}\cdot\pi(\mathbf{y})+P(\mathbf{y}), \end{aligned}$$

where π is any permutation of $\mathbb{F}_p^{\frac{n}{2}}$ and $P:\mathbb{F}_p^{\frac{n}{2}}\to\mathbb{F}_p$ is arbitrary. Such a bent function is regular.

(ii) When p is odd and $n>1$, it is not known if the upper bound (4.11) is attainable. When p and n are both odd with $n\geqslant 3$, it is not known if the upper bound (4.14) is attainable.

(iii) When $n=1$ and p is odd, $f\in\mathscr{F}(\mathbb{F}_p,\mathbb{F}_p)$ is bent if and only if $\deg f=2$, as we see in the following theorem.

Theorem 4.6. *Let p be an odd prime. Then $f\in\mathscr{F}(\mathbb{F}_p,\mathbb{F}_p)$ is bent if and only if* $\deg f=2$. *All such bent functions are weakly regular.*

Proof. It was shown in [5] that quadratic function in $\mathscr{F}(\mathbb{F}_p,\mathbb{F}_p)$ are weakly regular bent functions [5, Theorem 2]. Thus it remains to show that if $f\in\mathscr{F}(\mathbb{F}_p,\mathbb{F}_p)$ is bent, then $\deg f=2$. When $p=3$, the claim is obviously true. Hence we assume $p\geqslant 5$.

Write

$$f(x) = a_1 x^{d_1} + a_2 x^{d_2} + \cdots + a_m x^{d_m}, \tag{4.17}$$

where $d_1 > d_2 > \cdots > d_m \geqslant 0$ and $0 \neq a_i \in \mathbb{F}_p$ $(1 \leqslant i \leqslant m)$. By Proposition 4.4, $d_1 \leqslant \frac{p+1}{2}$.

We claim that $d_1 \neq \frac{p+1}{2}$. Otherwise, through a suitable translation $x \mapsto x + a$ $(a \in \mathbb{F}_p)$, we may assume that in (4.17), $d_2 \leqslant d_1 - 2$, hence $d_1 + d_2 \leqslant p - 1$. If $d_2 \leqslant 1$, since $af(x) + bx + c$ is bent for all $a, b, c \in \mathbb{F}_p$ with $a \neq 0$, the power function $x^{\frac{p+1}{2}}$ would be bent. However, $x^{\frac{p+1}{2}}$ is not bent for $p \geqslant 5$: If $p \equiv 1 \pmod 4$,

$$\sum_{x \in \mathbb{F}_p} \zeta^{x^{(p+1)/2}} = 0,$$

since $\gcd(\frac{p+1}{2}, p-1) = 1$. If $p \equiv 3 \pmod 4$,

$$\begin{aligned}
\sum_{x \in \mathbb{F}_p} \zeta^{x^{(p+1)/2} + x} &= \frac{1}{2}\left[\sum_{x \in \mathbb{F}_p} \zeta^{(x^2)^{(p+1)/2} + x^2} + \sum_{x \in \mathbb{F}_p} \zeta^{(-x^2)^{(p+1)/2} + (-x^2)}\right] \\
&= \frac{1}{2}\left[\sum_{x \in \mathbb{F}_p} \zeta^{2x^2} + p\right] \\
&= \frac{1}{2}(p \pm i\sqrt{p}),
\end{aligned}$$

where $|\frac{1}{2}(p \pm i\sqrt{p})| \neq \sqrt{p}$. Therefore, we conclude that $d_2 \geqslant 2$. Since $v_p(\hat{f}(\mathbf{c})) = \frac{1}{2}$ for all $\mathbf{c} \in \mathbb{F}_p$, by Theorem 4.1, we have

$$\begin{aligned}
& v_p\left(\sum_{\substack{0 \leqslant t_1, \ldots, t_m \leqslant p-1 \\ t_1 d_1 \oplus \cdots \oplus t_m d_m = d_1 + d_2}} G(t_1) \cdots G(t_m) \omega(a_1^{t_1} \cdots a_m^{t_m})\right) \\
&= v_p(h_f(d_1 + d_2)) \\
&\geqslant -\frac{1}{2} + \frac{1}{p-1}(d_1 + d_2).
\end{aligned} \tag{4.18}$$

Since $(t_1, t_2, \ldots, t_m) = (1, 1, 0, \ldots, 0) \in \{0, 1, \ldots, p-1\}^m$ is the only choice such that $t_1 d_1 \oplus \cdots \oplus t_m d_m = d_1 + d_2$ and $t_1 + \cdots + t_m \leqslant 2$, the left-hand side of (4.18) equals

$$v_p(G(1)G(1)G(0) \cdots G(0)\omega(a_1^1 a_2^1 a_3^0 \cdots a_m^0)) = \frac{2}{p-1}.$$

Hence (4.18) gives

$$\frac{2}{p-1} \geqslant -\frac{1}{2}+\frac{1}{p-1}(d_1+d_2) \geqslant -\frac{1}{2}+\frac{1}{p-1}\left(\frac{p+1}{2}+2\right),$$

which is not true.

Thus we have proved that $d_1 \leqslant \frac{p-1}{2}$. Let $r = \lfloor \frac{p-1}{d_1} \rfloor$. Then $r \geqslant 2$ and $d_1 > \frac{p-1}{r+1}$. Again by Theorem 4.1, we have

$$\begin{aligned}\frac{r}{p-1} &= v_p\left(\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant p-1\\ t_1d_1\oplus\cdots\oplus t_md_m=rd_1}} G(t_1)\cdots G(t_m)\omega(a_1^{t_1}\cdots a_m^{t_m})\right)\\ &= v_p(h_f(rd_1))\\ &\geqslant -\frac{1}{2}+\frac{1}{p-1}rd_1\end{aligned}$$

which implies

$$d_1 \leqslant 1+\frac{1}{2}\frac{p-1}{r}. \tag{4.19}$$

Therefore, we have

$$d_1 \leqslant 1+\frac{1}{2}\frac{r+1}{r}\frac{p-1}{r+1} < 1+\frac{1}{2}\frac{r+1}{r}d_1.$$

Solving the above inequality, we have

$$d_1 < 2+\frac{2}{r-1}.$$

If $r \geqslant 3$, then $d_1 \leqslant 2$ and we are done. If $r = 2$, then $d_1 \leqslant 3$. If $d_1 = 3$, $\lfloor \frac{p-1}{3} \rfloor = 2$ forces $p = 7$. But then (4.19) would not hold. Therefore we must have $d_1 \leqslant 2$. □

Concerning Corollary 1.3, it is also natural to ask if there is a p-ary version. We give a positive answer for $p = 3$.

Lemma 4.7. (i) *$f \in \mathscr{F}(\mathbb{F}_3^n, \mathbb{F}_3)$ is a bent function if and only if $v_3(\hat{f}(\mathbf{c})) = \frac{n}{2}$ for all $\mathbf{c} \in \mathbb{F}_3^n$.*

(ii) *$f \in \mathscr{F}(\mathbb{F}_3^n, \mathbb{F}_3)$ is a weakly regular bent function if and only if $v_3(\hat{f}(0)) = \frac{n}{2}$ $v_3(\hat{f}(\mathbf{c}) - \hat{f}(0)) > \frac{n}{2}$ for all $\mathbf{c} \in \mathbb{F}_3^n$.*

Proof. (i) We only have to prove the "if" part. For each $\mathbf{c} \in \mathbb{F}_3^n$, we have $v_3(|\hat{f}(\mathbf{c})|^2) = n$. However, since $|\hat{f}(\mathbf{c})|^2 \in \mathbb{Z}[\zeta] \cap \mathbb{R}$ and $\mathbb{Z}[\zeta] \cap \mathbb{R} = \mathbb{Z}$, we must have $|\hat{f}(\mathbf{c})|^2 \geqslant 3^n$. The

Parseval formula $\sum_{\mathbf{c}\in\mathbb{F}_3^n}|\hat{f}(\mathbf{c})|^2 = 3^{2n}$ forces $|\hat{f}(\mathbf{c})|^2 = 3^n$ for all $\mathbf{c}\in\mathbb{F}_3^n$. Hence f is a bent function.

(ii) Again, we only have to prove the "if" part. By (i), f is bent. Let $\delta\in\mathbb{C}$ be a primitive 12th root of unity. By Property 8 of [5], for each $\mathbf{c}\in\mathbb{F}_3^n$, there exists $k\in\mathbb{Z}$ such that

$$\hat{f}(\mathbf{c}) = p^{\frac{n}{2}}\delta(-\zeta)^k.$$

f is weakly regular if and only if in the above equation, k is even for all $\mathbf{c}$ or k is odd for all $\mathbf{c}$. Suppose to the contrary that there exist $\mathbf{c}_1, \mathbf{c}_2\in\mathbb{F}_3^n$ such that $\hat{f}(\mathbf{c}_i) = p^{\frac{n}{2}}\delta(-\zeta)^{k_i}$ with $k_1\not\equiv k_2 \pmod 2$. Since $v_3(1+\zeta^{k_2-k_1}) = 0$, we have $v_3(\hat{f}(\mathbf{c}_1) - \hat{f}(\mathbf{c}_2)) = v_3(\hat{f}(\mathbf{c}_1)(1+\zeta^{k_2-k_1})) = \frac{n}{2}$, which is a contradiction. □

Theorem 4.8. *Let $f\in\mathscr{F}(\mathbb{F}_3^n, \mathbb{F}_3)$. Then f is a weakly regular bent function if and only if*

$$v_3(h_f(2,\ldots,2)) = \frac{n}{2} \tag{4.20}$$

and

$$v_3(h_f(\mathbf{u})) > -\frac{n}{2} + \frac{1}{2}(u_1 + \cdots + u_n) \tag{4.21}$$

for all $(2,\ldots,2)\neq\mathbf{u} = (u_1,\ldots,u_n)\in\{0,1,2\}^n$.

Proof. Combining Lemma 4.7(ii) and Corollary 4.3, we see that f is a weakly regular bent function if and only if $v_3(\hat{f}(0)) = \frac{n}{2}$ and (4.21) holds. However, with (4.21), Lemma 4.2 gives

$$v_3\left(h_f(2,\ldots,2) - \frac{1}{2^n}\hat{f}(0)\right) > \frac{n}{2}.$$

Thus with (4.21), $v_3(\hat{f}(0)) = \frac{n}{2}$ if and only if $v_3(h_f(2,\ldots,2)) = \frac{n}{2}$. □

Theorem 4.8 can be stated explicitly in terms of the coefficients of f.

Corollary 4.9. *Let $f\in\mathscr{F}(\mathbb{F}_3^n, \mathbb{F}_3)$ be of the form*

$$f(\mathbf{x}) = \mathbf{x}^{\mathbf{u}_1} + \cdots + \mathbf{x}^{\mathbf{u}_l} - \mathbf{x}^{\mathbf{u}_{l+1}} - \cdots - \mathbf{x}^{\mathbf{u}_m}, \quad \mathbf{x}\in\mathbb{F}_3^n,$$

where $\mathbf{u}_1, \ldots, \mathbf{u}_m \in \{0,1,2\}^n$ *are distinct. Then f is a weakly regular bent function if and only if*

$$v_3\left(\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant 2\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=(2,\ldots,2)}} 2^{-|\{k:t_k\neq 0\}|}(\sqrt{-3})^{t_1+\cdots+t_m}(-1)^{t_{l+1}+\cdots+t_m}\right)=\frac{n}{2}$$

and

$$v_3\left(\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant 2\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}}} 2^{-|\{k:t_k\neq 0\}|}(\sqrt{-3})^{t_1+\cdots+t_m}(-1)^{t_{l+1}+\cdots+t_m}\right) > -\frac{n}{2}+\frac{1}{2}(u_1+\cdots+u_n)$$

for all $(2,\ldots,2)\neq\mathbf{u}=(u_1,\ldots,u_n)\in\{0,1,2\}^n$.

Proof. For $p=3$ we have $G(0)=1$, $G(1)=\frac{\sqrt{-3}}{2}$ and $G(2)=\frac{-3}{2}$. Therefore for $\mathbf{u}=(u_1,\ldots,u_n)\in\{0,1,2\}^n$,

$$\begin{aligned} h_f(\mathbf{u}) &= \sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant 2\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}}} G(t_1)\cdots G(t_m)(-1)^{t_{l+1}+\cdots+t_m}\\ &= \sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant 2\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}}} 2^{-|\{k:t_k\neq 0\}|}(\sqrt{-3})^{t_1+\cdots+t_m}(-1)^{t_{l+1}+\cdots+t_m}. \end{aligned}$$

Thus the corollary is a restatement of Theorem 4.8. □

Acknowledgments

Research supported by NSA Grant MDA 904-02-1-0080.

References

[1] J. Ax, Zeros of polynomials over finite fields, Amer. J. Math. 86 (1964) 255–261.
[2] C. Carlet, Generalized partial spreads, IEEE Trans. Inform. Theory 41 (1995) 1482–1487.
[3] C. Carlet, P. Guillot, A new representation of Boolean functions, Lecture Notes in Computer Science, Vol. 1719, Springer, New York, 1999, pp. 94–103.
[4] C. Carlet, P. Guillot, Bent, resilient functions and the numerical normal form, in Codes and Association Schemes, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Vol. 56, American Mathematical Society, Providence, RI, 2001, pp. 87–96.

[5] P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties, J. Combin. Theory A 40 (1985) 90–107.
[6] S. Lang, Algebraic Number Theory, Springer, New York, 1986.
[7] S. Lang, Cyclotomic Fields, I and II, Springer, New York, 1990.
[8] P. Langevin, On generalized bent functions, Eurocode '92 (Udine, 1992), CISM Courses and Lectures, Vol. 339, Springer, Vienna, 1993, pp. 147–157.
[9] O.S. Rothaus, On "bent" functions, J. Combin. Theory A 20 (1976) 300–305.
[10] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inform. Theory 30 (1984) 776–780.